

Импортозамещенная ИТ-инфраструктура (виртуализация и ОС): анализ текущих подходов к защите и тренды

Сергей Кузнецов

Коммерческий директор
ЦЕНТРА ЗАЩИТЫ ИНФОРМАЦИИ
ООО «КОНФИДЕНТ»

EMAIL: ksp@CONFIDENT.RU

WEB: WWW.DALLASLOCK.RU



Про что эта презентация

- Востребованность несертифицированных ОС/ВИ в «связке» с наложенными СЗИ
- Новый тренд – использование сертифицированных ОС/ВИ в «связке» с наложенными СЗИ
- «Плюсы» и «минусы» разных подходов к защите информации. Рекомендации вендора по выбору подхода реализации мер защиты на объекте



Откуда мы это взяли

- Аналитический обзор госзакупок (ГК «Конфидент»)
- Участие в ТК362 и в других структурах с целью разработки нормативной базы ИБ
- Опыт специалистов ГК «Конфидент» – 31 год на рынке, более 5500 проектов в год
- Опыт партнеров ГК «Конфидент» (около 600), в том числе по аттестации



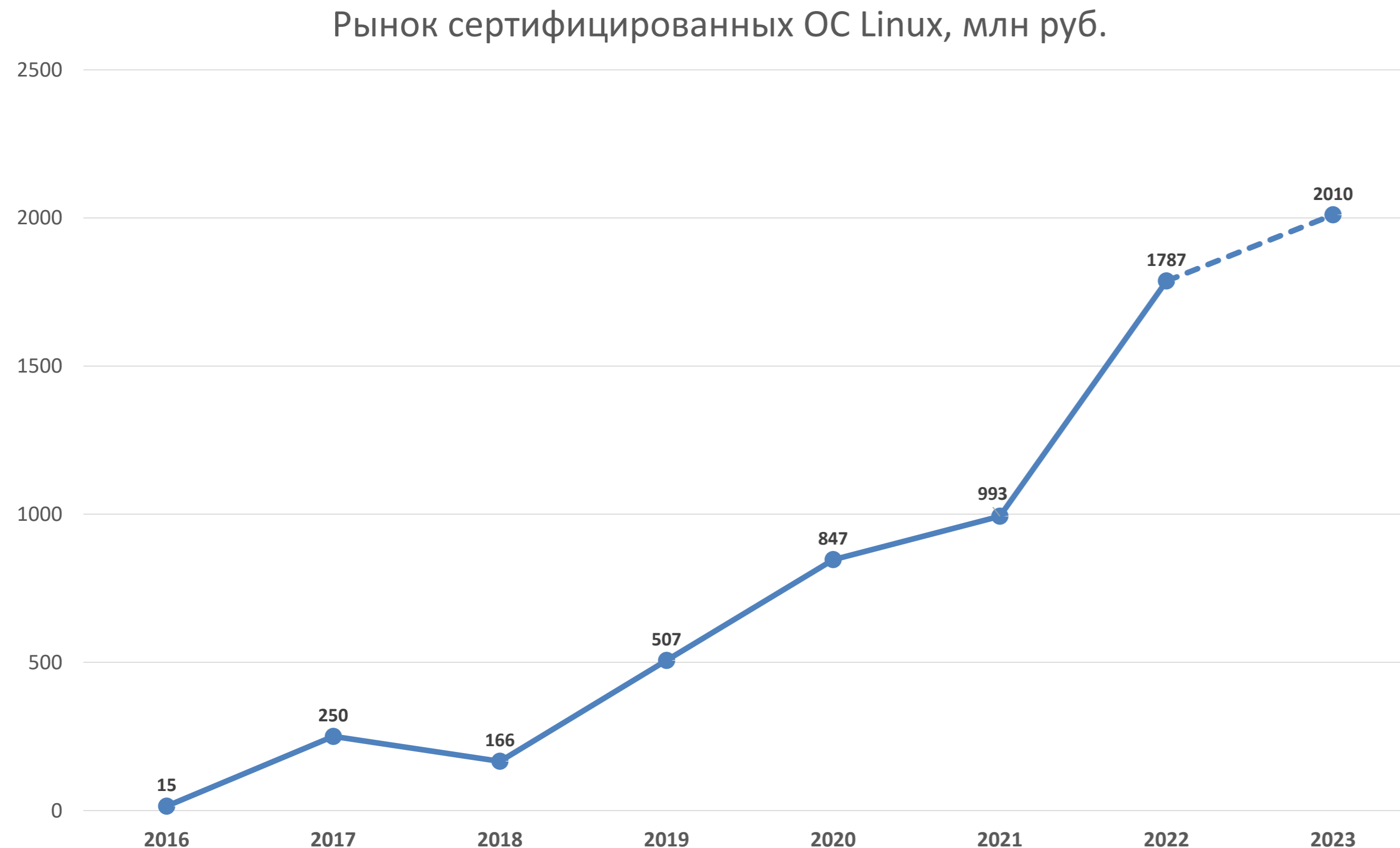
Документы для участников конференции

- Презентация
- Брошюра «Преимущества наложенных СЗИ»
- Аналитический документ «Преимущества и недостатки сертифицированных ОС и наложенных СЗИ»
- Лабораторные практикумы по установке и администрированию СЗИ Dallas Lock (8.0, Linux, СДЗ, СЗИ ВИ, ЕЦУ)



Импортозамещенная физическая ИТ инфраструктура – ОС

Рынок сертифицированных ОС Linux



Уверенный рост рынка с 2019 года



В 2023 «Русбитех-Астра» планирует удвоить доходы

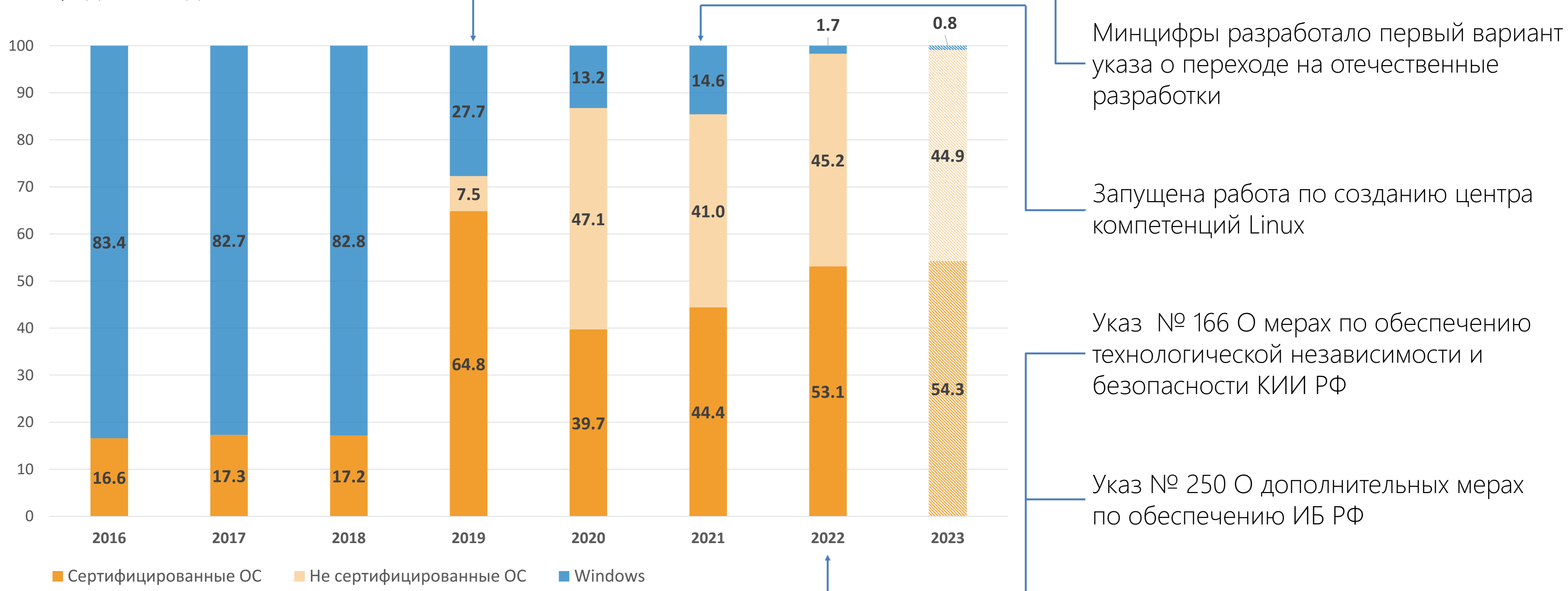


В 2023 «Базальт СПО» ожидает рост на 30%.

Результаты получены из аналитического обзора «Анализ государственных закупок» ЦЗИ ГК «Конфидент»

Доли различных типов ОС

Распределение долей, %



Результаты получены из аналитического обзора «Анализ государственных закупок» ЦЗИ ГК «Конфидент»

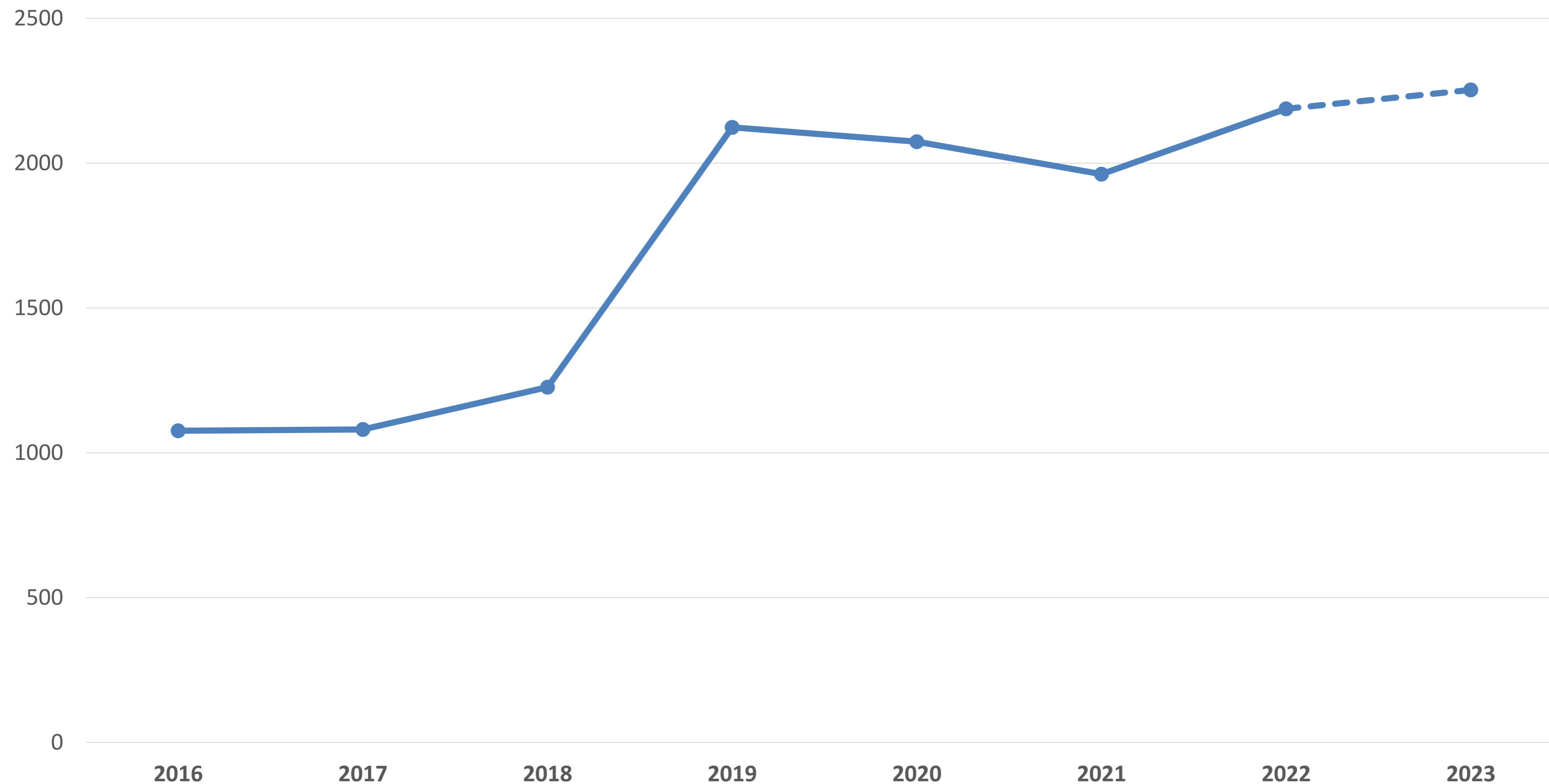
Сертифицированные ОС Linux

- Мандатное разграничение доступа
- Ниже вероятность обнаружения уязвимостей
- Объединение ролей ИБ и ИТ
- Встроенные системы защиты настроены «из коробки»

- Отсутствие интеграции в инфраструктуру безопасности
- Отсутствие межсетевого экрана уровня хоста
- Совместимость сертифицированных ОС с прикладным ПО
- Высокая стоимость не только внедрения, но и совокупная стоимость владения в долгосрочной перспективе

Рынок наложенных (накладных) СЗИ

Рынок СЗИ НДС для ОС Windows, млн руб.



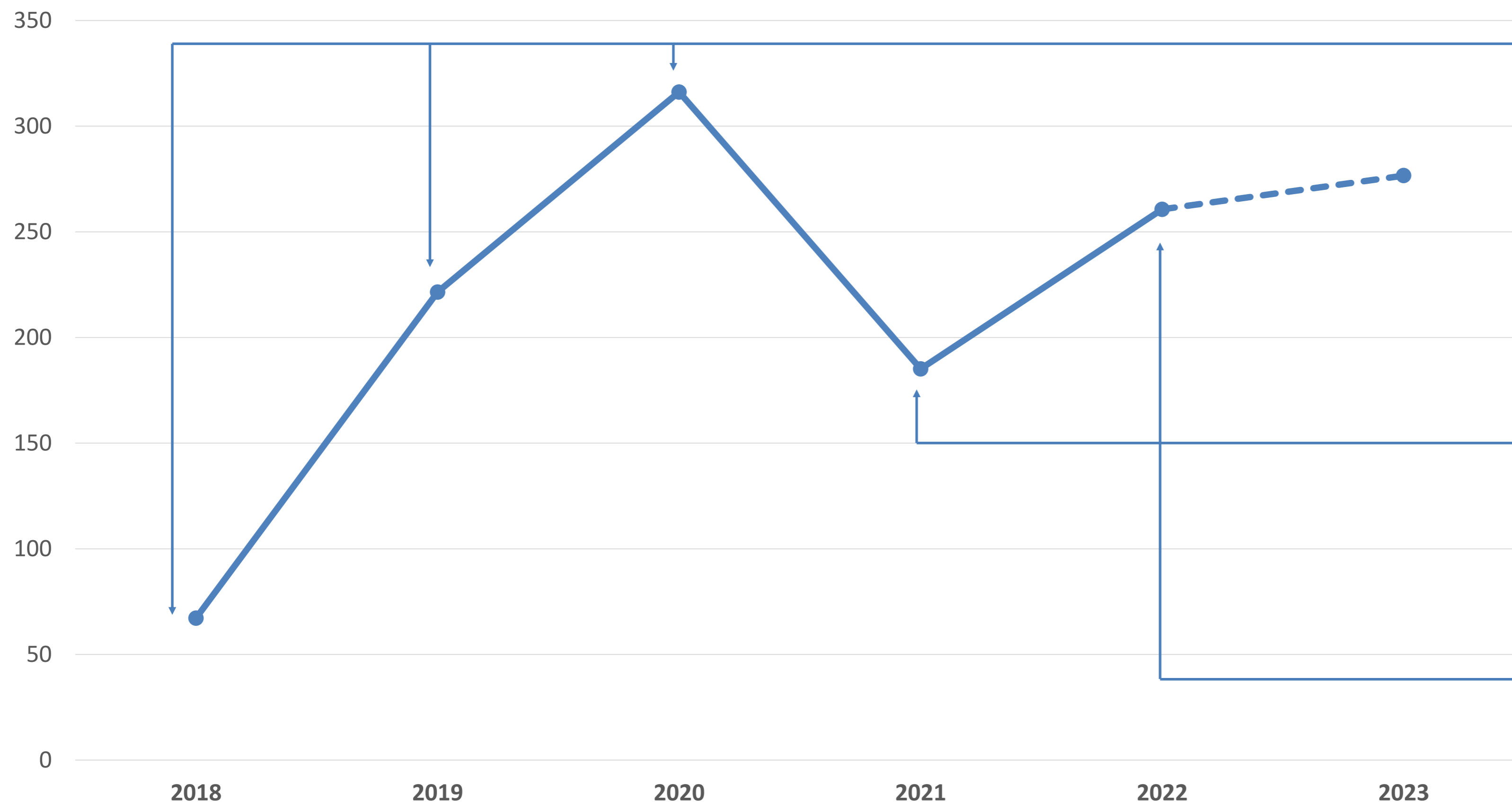
Рынок СЗИ НДС для ОС Windows HE сокращается

СЗИ НДС для ОС Windows реально используется

Результаты получены из аналитического обзора «Анализ государственных закупок» ЦЗИ ГК «Конфидент»

Рынок наложенных (накладных) СЗИ

Рынок СЗИ НДС для ОС Linux, млн руб.



Стабильный рост СЗИ НДС. Быстрое внедрение, понятная модель безопасности, легкость интегрирования с уже существующими системами

Рынок отечественных сертифицированных ОС оказывает серьезное влияние, особенно в условиях активного импортозамещения

Доля несертифицированных ОС не сокращалась, а следовательно стимулировала рост СЗИ НДС для ОС Linux

Результаты получены из аналитического обзора «Анализ государственных закупок» ЦЗИ ГК «Конфидент»

Сертифицированная ОС ?



Несертифицированная ОС + наложенные СЗИ ?



Сертифицированная ОС + наложенные СЗИ ?

Преимущества наложенных СЗИ

Решение конкретных задач по защите ИБ

- модульность СЗИ НСД
- целенаправленное закрытие уязвимостей в соответствии с моделью угроз

Реализация быстрого внедрения

- быстрая установка и настройка СЗИ НСД
- удобное масштабирование

Высокая совместимость

- отсутствие проблем с зависимостями
- легко интегрируются с уже существующими системами

Экономия бюджета

- накладные решения дешевле
- ниже совокупная стоимость владения СЗИ
- проще обслуживать и поддерживать







Функциональные преимущества

- централизованное управление
- управление правилами встроенного в ОС межсетевого экрана
- межсетевой экран уровня узла согласно «ИТ.МЭ.В4.ПЗ»
- отдельный модуль «СКН подключения» согласно «ИТ.СКН.П4.ПЗ»
- возможность разделения ролей администратора ИБ и администратора ИТ









Сканируйте.
Сохраняйте.







Наложенные СЗИ или сертифицированные ОС на объекте под аттестацию

Меры защиты ФСТЭК России	Серт. ОС	Наложен-ные СЗИ
<p>УПД.2. Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), ТИПОВ (чтение, запись, выполнение или иной тип) и правил разграничения доступа</p>		
<p>УПД.3. Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами ИС, а также между ИС</p>		
<p>ОПС.1. Управление запуском (обращениями) компонентов программного обеспечения</p>		

Наложенные СЗИ или сертифицированные ОС на объекте под аттестацию

Меры защиты ФСТЭК России	Серт. ОС	Наложен-ные СЗИ
АУД.4. Генерирование временных меток и (или) синхронизация системного времени АУД.8. Реагирование на сбои при регистрации событий безопасности		
ОДТ.6. Кластеризация информационной системы и (или) её сегментов		
ЗНИ.5. Контроль использования интерфейсов ввода (вывода) информации на машинные носители персональных данных		

Наложенные СЗИ или сертифицированные ОС на объекте под аттестацию

Меры защиты ФСТЭК России	Серт. ОС	Наложен-ные СЗИ
ЗИС.7. Контроль санкционированного и исключение несанкционированного использования технологий мобильного кода, в том числе регистрация событий, их анализ и реагирование на нарушения		
ЗИС.19. Изоляция процессов (выполнение программ) в выделенной области памяти		
ЗИС.38. Защита информации при использовании мобильных устройств		

Наложенные СЗИ + сертифицированные ОС – новый тренд



Плановый внутренний релиз СЗИ НСД Dallas Lock Linux – конец декабря 2023 года

РАЗРАБОТКА



Импортозамещенная виртуальная ИТ инфраструктура – ВИ

Рынок платформ виртуализации



Уход зарубежных вендоров сильно сказался на объеме рынка

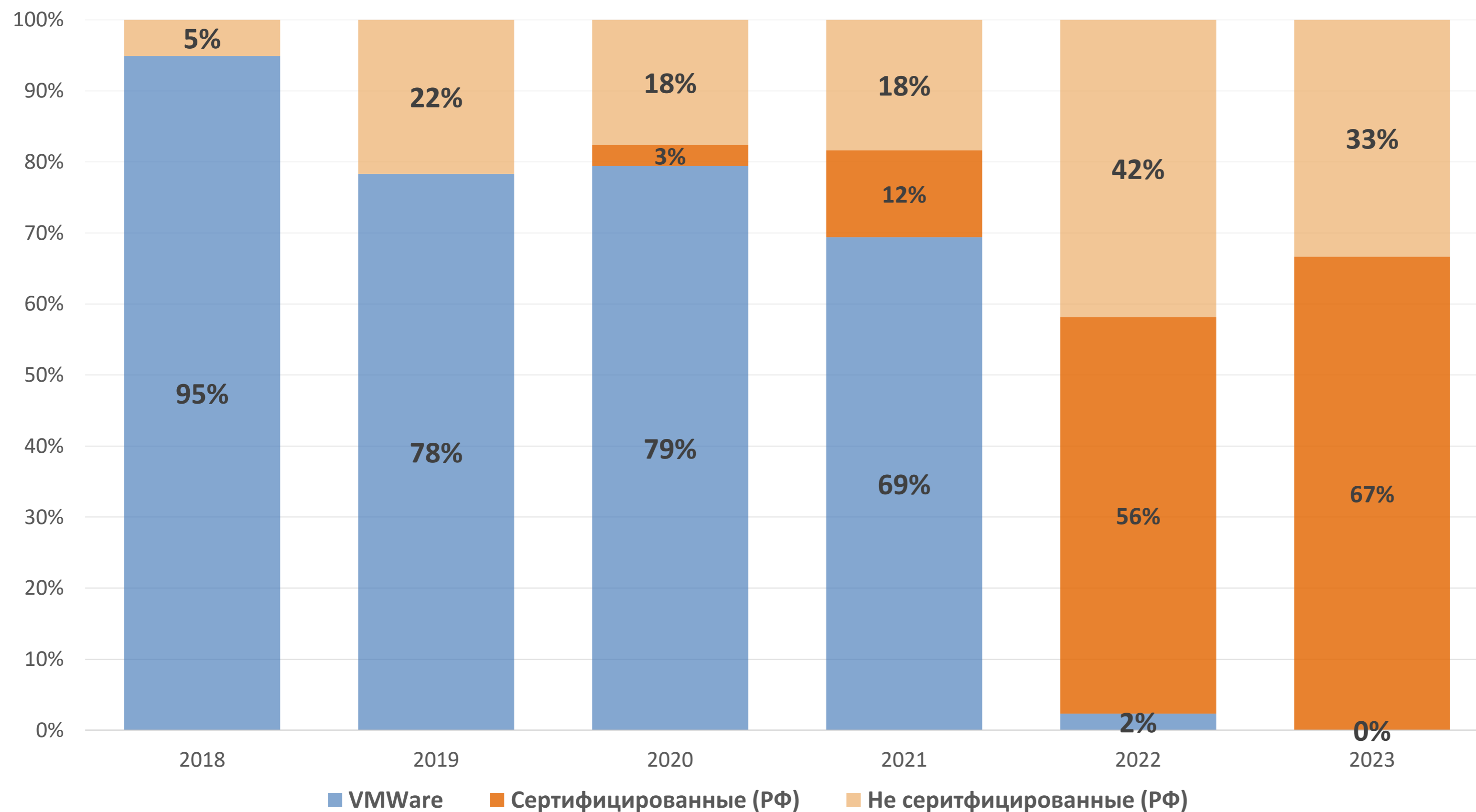
2020-2021 годы лидирующую позицию на рынке среди средств серверной виртуализации занимали решения:

- VMware – 95%
- Hyper-V – 4.6%
- отечественные решения – 0.4%

Результаты получены из аналитического обзора «Анализ государственных закупок» ЦЗИ ГК «Конфидент»

Доли различных типов платформ виртуализации

Распределение долей, %

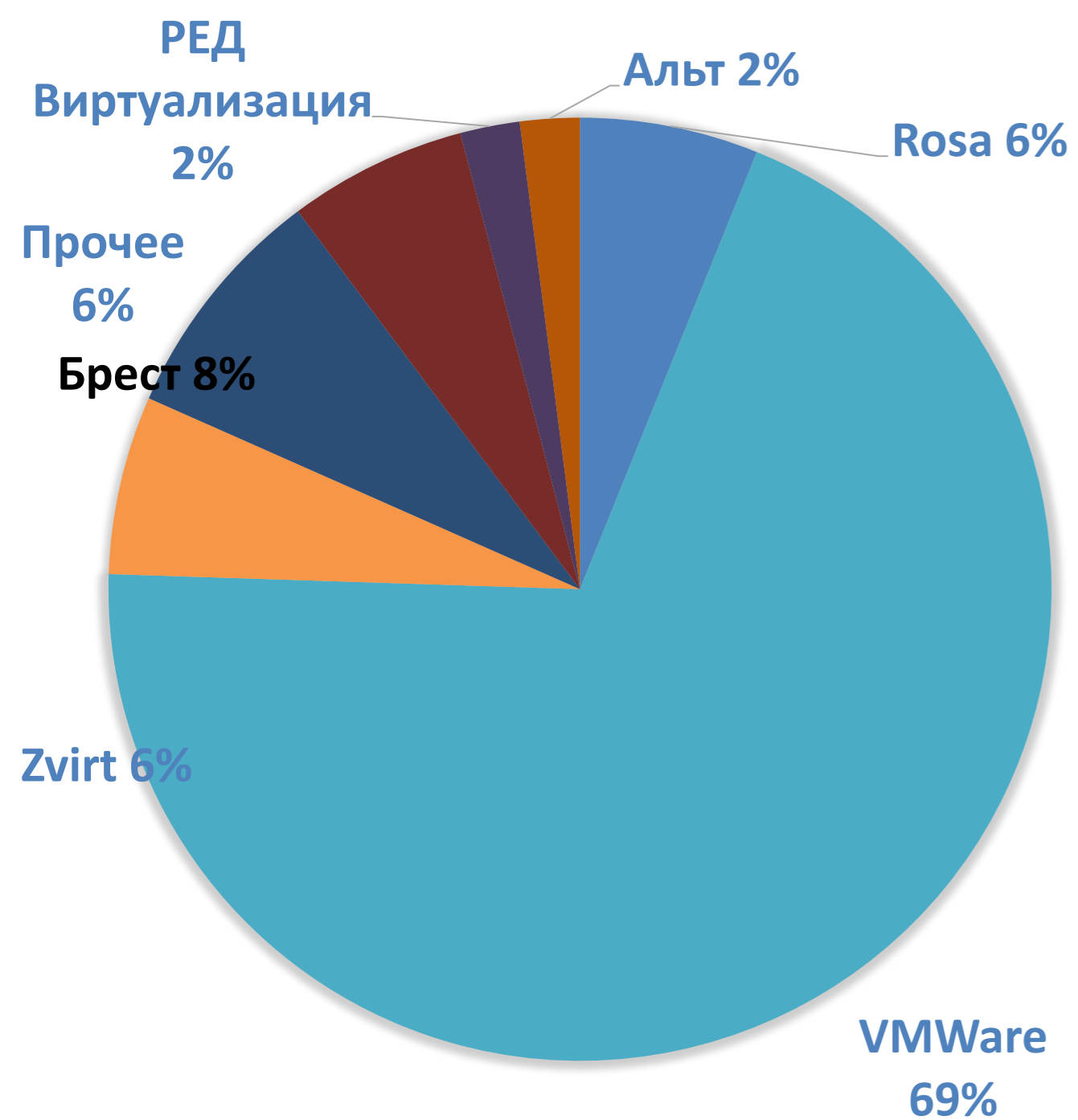


Участники рынка:

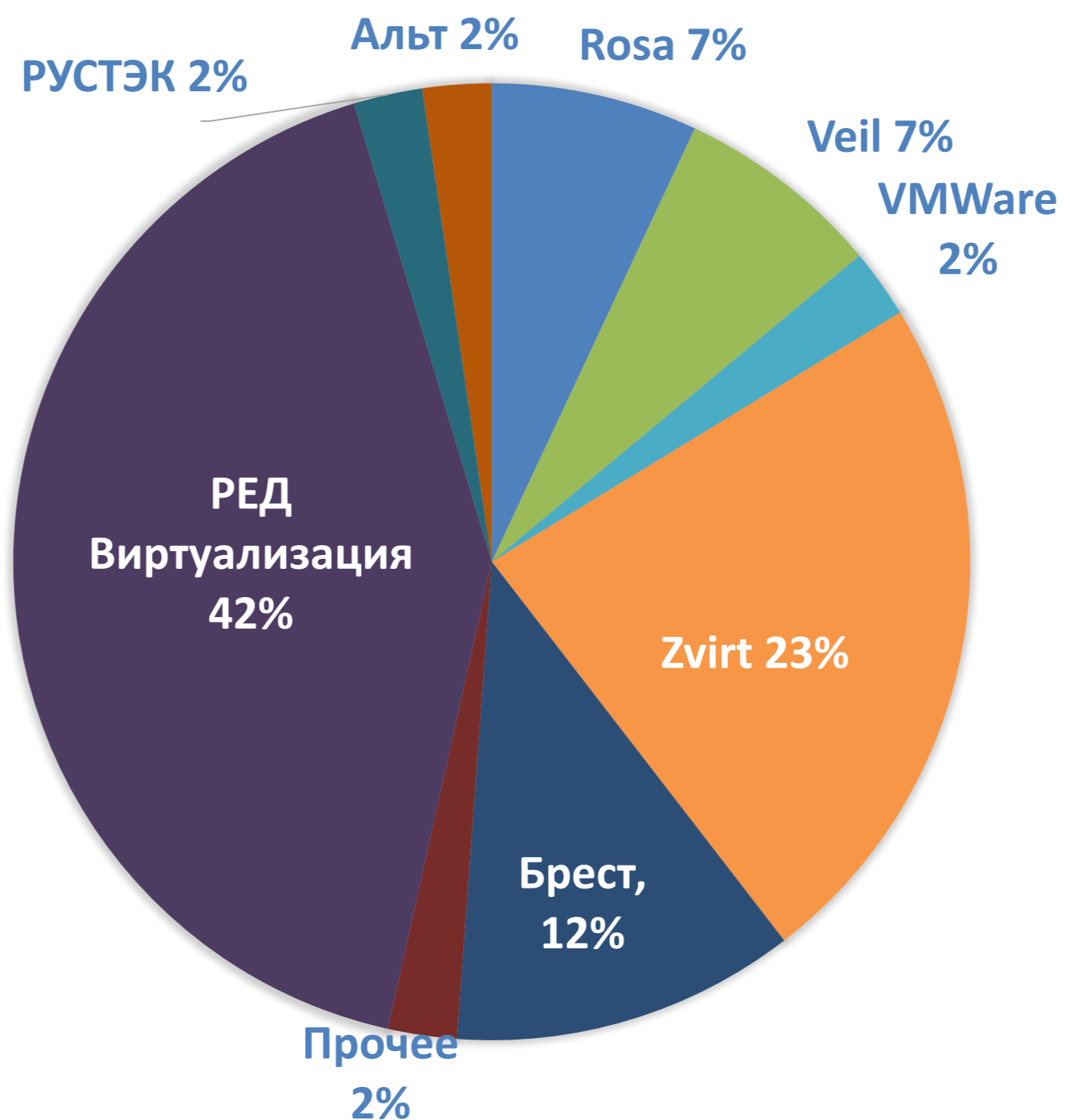
- VMWare (до 2022 года)
- Rosa (НТЦ ИТ РОСА)
- Zvirt (Orion soft)
- РЕД Виртуализация (ООО «РЕД СОФТ»)
- Брест РусБИТех-Астра (ГК Астра)
- Альт (Базальт СПО)
- Р-Виртуализация (Росплатформа)
- Veil (НИИ Масштаб)
- РУСТЭК (РУСТЭК)
- VMmanager («ИСПсистем» (ГК «Астра»))

Результаты получены из аналитического обзора «Анализ государственных закупок» ЦЗИ ГК «Конфидент»

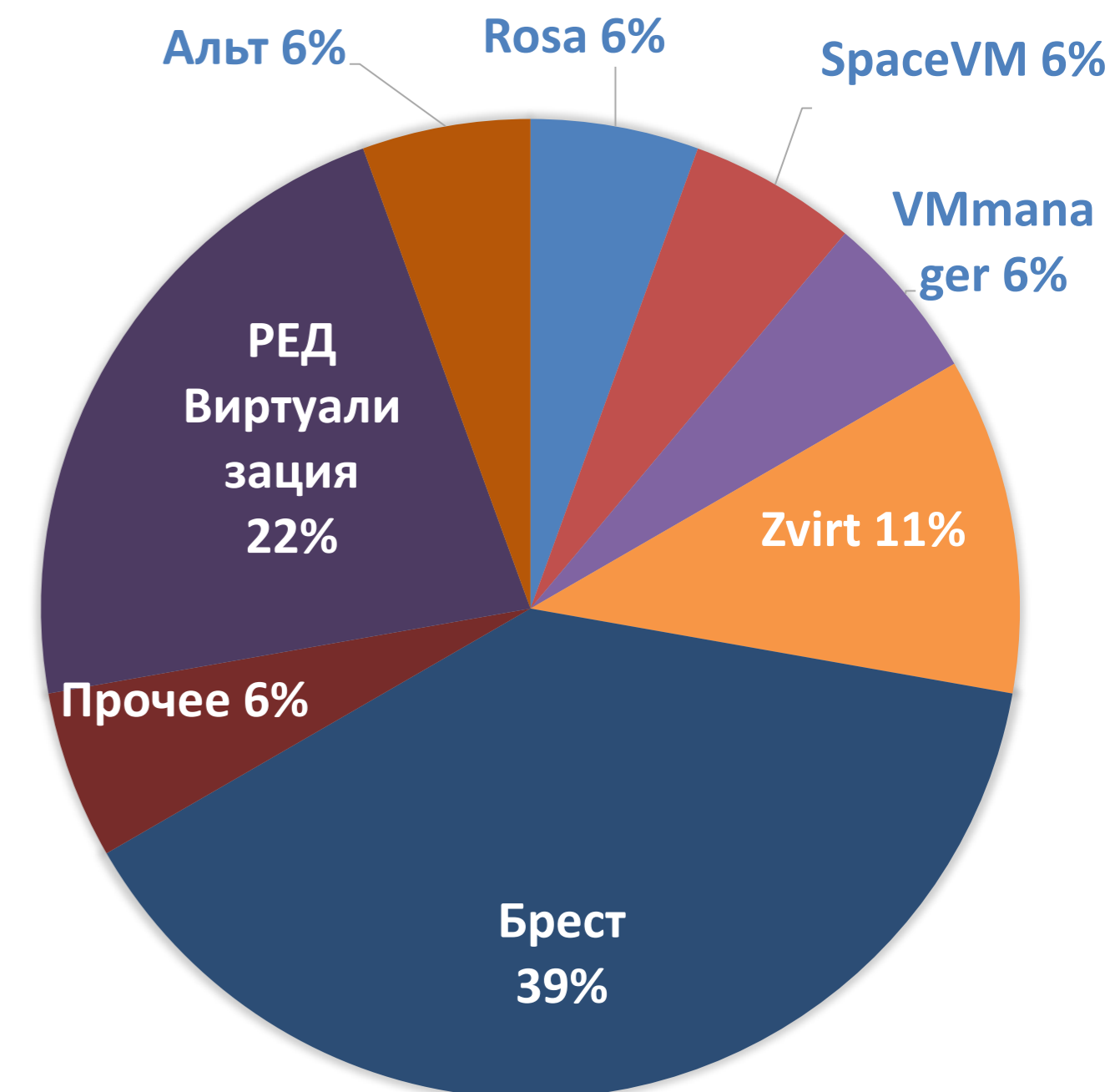
Отсутствие явных лидеров платформ виртуализации в 2022-2023



2021



2022

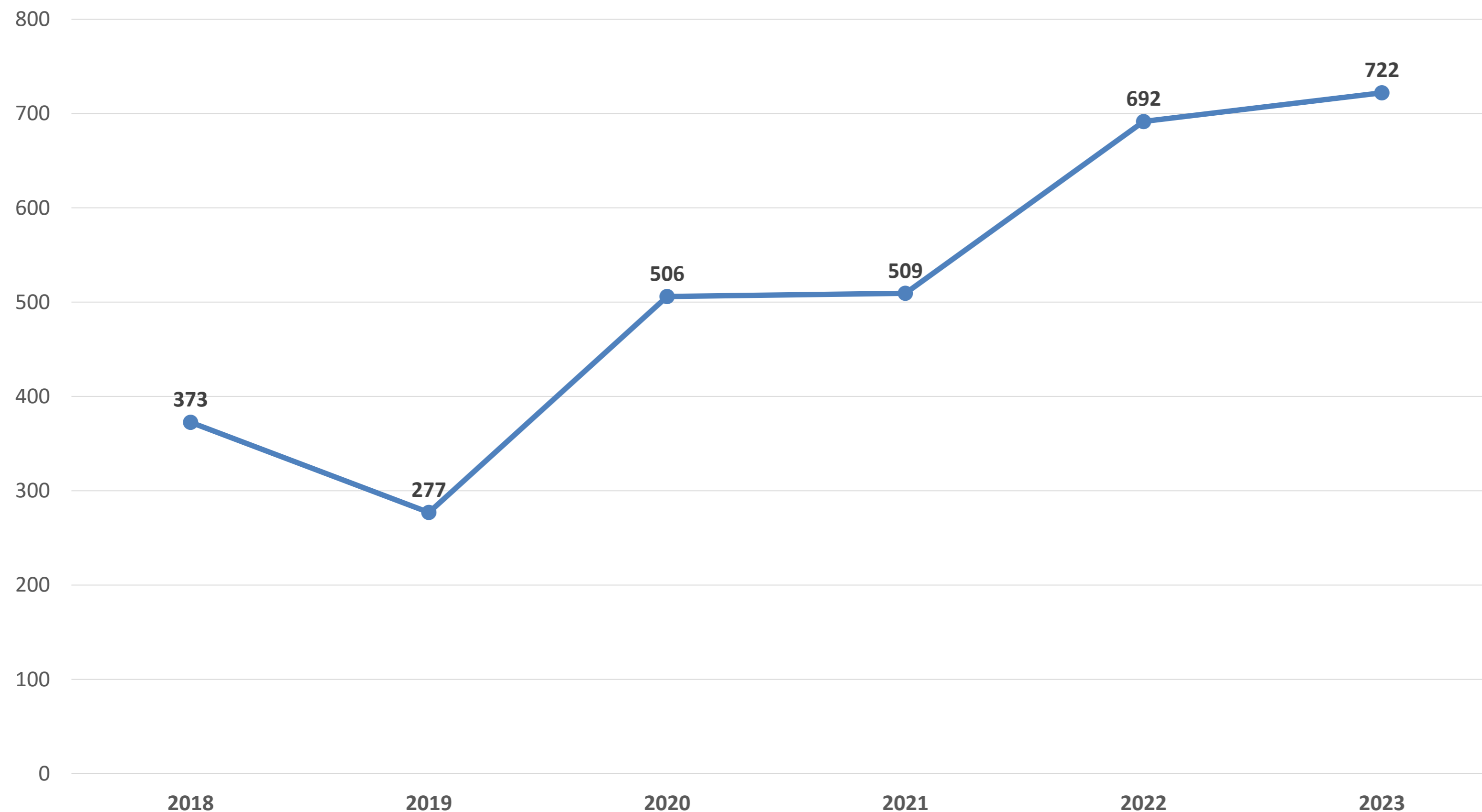


2023

Результаты получены из аналитического обзора «Анализ государственных закупок» ЦЗИ ГК «Конфидент»

Рынок накладных решений для виртуализации

Рынок накладных решений, млн руб.



Рынок накладных средств защиты информации все еще в фазе роста и не сокращается

Участники рынка:

- vGate (Код безопасности)
- СЗИ ВИ Dallas Lock (Конфидент)

Результаты получены из аналитического обзора «Анализ государственных закупок» ЦЗИ ГК «Конфидент»



Про что была эта презентация

- Востребованность несертифицированных ОС/ВИ в «связке» с наложенными СЗИ
- Новый тренд – использование сертифицированных ОС/ВИ в «связке» с наложенными СЗИ
- «Плюсы» и «минусы» разных подходов к защите информации. Рекомендации вендора по выбору подхода реализации мер защиты на объекте

Спасибо за внимание!

EMAIL: ksp@CONFIDENT.RU

WEB: WWW.DALLASLOCK.RU